

SUPERSINGULAR GENUS-TWO CURVES OVER FIELDS OF CHARACTERISTIC THREE

EVERETT W. HOWE

ABSTRACT. Let C be a supersingular genus-2 curve over an algebraically closed field of characteristic 3. We show that if C is not isomorphic to the curve $y^2 = x^5 + 1$ then up to isomorphism there are exactly 20 degree-3 maps φ from C to the elliptic curve E with j -invariant 0. We study the coarse moduli space of triples (C, E, φ) , paying particular attention to questions of rationality. The results we obtain allow us to determine, for every finite field k of characteristic 3, the polynomials that occur as Weil polynomials of supersingular genus-2 curves over k .

1. INTRODUCTION

Over an algebraically closed field of characteristic 3, every supersingular genus-2 curve C has a degree-3 map to the supersingular elliptic curve E with j -invariant 0. We study the coarse moduli space \mathcal{A} of such maps $C \rightarrow E$, paying special attention to questions of rationality. We show that with a single exception, every supersingular genus-2 curve over an algebraically-closed field of characteristic 3 has 20 non-isomorphic maps to the elliptic curve with j -invariant 0, and we provide explicit equations for these maps.

Our motivation for studying these maps is the question of determining which isogeny classes of abelian surfaces over a finite field contain Jacobians. Much has been written on this question [1, 3, 4, 5, 6, 9, 13, 14, 15, 16, 18, 19], and together the works just cited answer the question for all simple non-supersingular isogeny classes. In recent joint work [10], Enric Nart, Christophe Ritzenthaler, and the author developed techniques to address the non-simple isogeny classes and the supersingular isogeny classes, thus completing the determination of the isogeny classes of abelian surfaces over finite fields that contain Jacobians. However, to avoid various special cases, the arguments in [10] concerning supersingular isogeny classes assume that the characteristic of the base field is larger than 3. The characteristic 2 case is dealt with in [15]. In this paper, we use our results on the moduli space \mathcal{A} to answer the question for supersingular isogeny classes in characteristic 3. We obtain the following theorem:

Theorem 1.1. *Let $q = 3^d$ be a power of 3. If d is odd, then the polynomials that occur as the Weil polynomials of supersingular genus-2 curves over \mathbb{F}_q are:*

- (1) $(x^2 + q)(x^2 - sx + q)$ for all $s \in \{\pm\sqrt{3q}\}$;
- (2) $(x^2 + q)^2$, if $q > 3$;

Date: 18 April 2006.

2000 Mathematics Subject Classification. Primary 11G20; Secondary 14G10, 14G15.

Key words and phrases. Curve, Jacobian, supersingular, abelian surface, zeta function, Weil polynomial, Weil number.

- (3) $x^4 + q^2$;
- (4) $x^4 + qx^2 + q^2$;
- (5) $x^4 - 2qx^2 + q^2$, if $q > 3$.

If d is even, the polynomials that occur as the Weil polynomials of supersingular genus-2 curves over \mathbb{F}_q are:

- (1) $(x^2 - 2sx + q)(x^2 + sx + q)$ for all $s \in \{\pm\sqrt{q}\}$;
- (2) $(x^2 - sx + q)^2$ for all $s \in \{0, \pm\sqrt{q}\}$;
- (3) $(x^2 - 2sx + q)^2$ for all $s \in \{\pm\sqrt{q}\}$, if $q > 9$;
- (4) $x^4 + q^2$;
- (5) $x^4 - sx^3 + qx^2 - sqx + q^2$ for all $s \in \{\pm\sqrt{q}\}$.

To prove these results, we show that the moduli space \mathcal{A} is isomorphic to the coarse moduli space \mathcal{B} of pairs (C, G) , where C is a supersingular genus-2 curve in characteristic 3 and G is an order-4 subgroup of $(\text{Jac } C)[2]$ that is not isotropic with respect to the Weil pairing. We give explicit models for these moduli spaces, as well as for the maps from these spaces to the moduli space of supersingular genus-2 curves in characteristic 3.

In Section 2 we provide some basic facts about supersingular genus-2 curves in characteristic 3; in particular, we show that the coarse moduli space \mathcal{S} of such curves is isomorphic to the affine line. In Section 3 we classify the degree-3 maps from supersingular genus-2 curves to the j -invariant 0 elliptic curve in characteristic 3. We show that the coarse moduli space \mathcal{A} of such maps is isomorphic to the affine line with one point removed, and that the natural map $\mathcal{A} \rightarrow \mathcal{S}$ has degree 20. In Section 4 we give complete lists of the isomorphism classes of supersingular elliptic curves over every finite field of characteristic 3, and we calculate the Weil polynomial of each isomorphism class. Finally, in Section 5 we use the results of the earlier sections to determine which isogeny classes of supersingular abelian surfaces in characteristic 3 do not contain Jacobians, thereby proving Theorem 1.1.

Notation. If X is a scheme over a field K , and if L is an extension field of K , we let X_L denote the base extension of X to L .

Acknowledgments. The author is grateful to Enric Nart and Christophe Ritzenthaler for encouragement and helpful discussions.

2. BASIC FACTS ABOUT SUPERSINGULAR GENUS-TWO CURVES IN CHARACTERISTIC THREE.

In this section we determine the locus of supersingular genus-2 curves in characteristic 3, viewed as a subvariety of the coarse moduli space of genus-2 curves.

If k is a field, we set $S_k = \mathbb{A}_k^5 \setminus \{[0, 0, 0, 0, 0]\}$ and we let W be the orbit space of S_k under the action of k^* defined by

$$\lambda[x_1, x_2, x_3, x_4, x_5] = [\lambda^2 x_1, \lambda^4 x_2, \lambda^6 x_3, \lambda^8 x_4, \lambda^{10} x_5],$$

so that W is a weighted projective space. We denote the orbit of $[x_1, x_2, x_3, x_4, x_5]$ by $[x_1 : x_2 : x_3 : x_4 : x_5]$. Igusa [12] associated to every genus-2 curve over k an element $[J_2 : J_4 : J_6 : J_8 : J_{10}]$ of W such that $J_{10} \neq 0$ and $4J_8 = J_2 J_6 - J_4^2$. This element is the *vector of Igusa invariants* of the curve. Igusa showed that over an algebraically closed field, every element of W with $J_{10} \neq 0$ and $4J_8 = J_2 J_6 - J_4^2$ comes from a genus-2 curve, and two genus-2 curves have the same vector of Igusa invariants if and only if they are isomorphic to one another. (Note, however, that a

point of this variety that is rational over a subfield of k does not always come from a curve defined over that field.) Thus, Igusa determined the coarse moduli space \mathcal{M}_2 of genus-2 curves.

Theorem 2.1. *Let k be a field of characteristic 3.*

- (a) *Let C be a genus-2 curve over k and let $[J_2 : J_4 : J_6 : J_8 : J_{10}]$ be its vector of Igusa invariants. Then C is supersingular if and only if $J_2 = J_4 = J_8 = 0$.*
- (b) *Let A and B be elements of k , with $B \neq 0$. Then the curve*

$$y^2 = x^6 + Ax^3 + Bx + A^2$$

is a supersingular curve of genus 2, and its vector of Igusa invariants is equal to $[0 : 0 : A : 0 : B]$.

Proof. First we dispose of an annoying special case. Suppose $k = \mathbb{F}_3$ and C is the curve $y^2 = x^5 - x$. Then C is not supersingular (because its Weil polynomial is $t^4 - 2t^2 + 9$) and its vector of Igusa invariants is $[1 : 0 : -1 : -1 : -1]$.

If k is larger than \mathbb{F}_3 , or if C is any curve other than $y^2 = x^5 - x$, then C has a model over k of the form $dy^2 = x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + c_0$, where the polynomial in x is separable. Now we use the criterion for supersingularity given in [20, Lemma E, p. 387]: Let M and $M^{(3)}$ be the matrices

$$M = \begin{bmatrix} c_2 & c_1 \\ c_5 & c_4 \end{bmatrix} \quad M^{(3)} = \begin{bmatrix} c_2^3 & c_1^3 \\ c_5^3 & c_4^3 \end{bmatrix}.$$

Then C is supersingular if and only if $MM^{(3)} = 0$, and the Jacobian of C is isomorphic to a product of supersingular elliptic curves (that is, the Jacobian is *superspecial*) if and only if $M = 0$. (Actually, to apply [20, Lemma E, p. 387] we should write our curve as $y^2 = (\text{quintic})$. However, the proof in [20] works for curves of the form $y^2 = (\text{sextic})$ as well.)

We note in passing that $M \neq 0$, because a polynomial of the form $x^6 + c_3x^3 + c_0$ is not separable. This shows that there are no superspecial genus-2 curves in characteristic 3, as we know already from [11, Prop. 3.1].

Note that

$$MM^{(3)} = \begin{bmatrix} c_2^4 + c_1c_5^3 & c_2c_1^3 + c_1c_4^3 \\ c_5c_2^3 + c_4c_5^3 & c_5c_1^3 + c_4^4 \end{bmatrix}.$$

Suppose the curve is supersingular, so that this matrix is the zero matrix. If $c_5 = 0$ then we must have $c_4 = c_2 = 0$, so C can be written in the form $dy^2 = x^6 + c_3x^3 + c_1x + c_0$. On the other hand, if c_5 is nonzero then we can translate x by a constant in order to get a new equation for C of the form $dy^2 = x^6 + c_5x^5 + c_3x^3 + c_2x^2 + c_1x + c_0$. Then we find that $c_2 = c_1 = 0$, so C is of the form $dy^2 = x^6 + c_5x^5 + c_3x^3 + c_0$. If we replace x with $1/x$ and rescale y , we find that we can again write C in the form $dy^2 = x^6 + c_3x^3 + c_1x + c_0$.

One can calculate that the Igusa invariants of the curve $dy^2 = x^6 + c_3x^3 + c_1x + c_0$ are $[0 : 0 : c_3^6 - c_3c_1^3 - c_0^3 : 0 : -c_1^6]$. (The computer algebra system Magma [2] provides facilities for calculating Igusa invariants.) This proves the ‘only if’ part of statement (a).

If we take $c_3 = A$, $c_1 = B$, $c_0 = A^2$, and $d = 1$, we find that the Igusa invariants are $[0 : 0 : -AB^3 : 0 : -B^6] = [0 : 0 : A : 0 : B]$. Thus, any curve with $J_2 = J_4 = J_8 = 0$ is geometrically isomorphic to one of the form $y^2 = x^6 + Ax^3 + Bx + A^2$, and the criterion from [20] shows that this curve is supersingular. This proves statement (b) and the ‘if’ part of statement (a). \square

Given a supersingular genus-2 curve C over a field of characteristic 3, we let $I_C = J_6^5/J_{10}^3$, where $[0 : 0 : J_6 : 0 : J_{10}]$ is the vector of Igusa invariants of C .

Theorem 2.2. *Let k be a field of characteristic 3.*

(a) *The map*

$$\left\{ \begin{array}{c} k\text{-isomorphism classes of} \\ \text{supersingular genus-2 curves over } k \end{array} \right\} \rightarrow k$$

that sends C to I_C is surjective, and is bijective if k is algebraically closed.

(b) *If c is a nonzero element of k , then the curve C defined by*

$$y^2 = x^6 + c^2x^3 + c^3x + c^4$$

is supersingular and satisfies $I_C = c$. The curve C defined by $y^2 = x^5 + 1$ is supersingular and satisfies $I_C = 0$.

(c) *Let C be a supersingular genus-2 curve over k . The geometric automorphism group of C has order 2 if $I_C \neq 0$, and order 10 if $I_C = 0$.*

Proof. Given any nonzero c , let C be the curve $y^2 = x^6 + c^2x^3 + c^3x + c^4$. It is easy to check that $I_C = c$. Likewise, it is easy to check that the Igusa invariants of the curve C defined by $y^2 = x^5 + 1$ are $[0 : 0 : 0 : 0 : 1]$, so we have $I_C = 0$. This proves statement (b) and the surjectivity claim of statement (a).

Suppose C and C' are supersingular genus-2 curves, with Igusa invariants $[0 : 0 : A : 0 : B]$ and $[0 : 0 : A' : 0 : B']$, respectively. Then $I_C = A^5/B^3$ and $I_{C'} = (A')^5/(B')^3$. Let λ be a 10th root of B'/B . If $I_C = I_{C'}$ then we have $(A')^5 = \lambda^{30}A^5$, so $A' = \zeta\lambda^6A$ for some 5-th root of unity ζ . If we replace λ with λ/ζ , then we have $B' = \lambda^{10}B$ and $A' = \lambda^6A$, so $[0 : 0 : A : 0 : B] = [0 : 0 : A' : 0 : B']$, and C and C' are geometrically isomorphic to one another. This proves the bijectivity claim of statement (a).

Finally, we note that Igusa [12, §8] calculated the automorphism groups of all genus-2 curves in every characteristic. In characteristic 3, the only curve with automorphism group larger than $\{\pm 1\}$ is the curve with Igusa invariants $[0 : 0 : 0 : 0 : 1]$, whose automorphism group is cyclic of order 10. This proves statement (c). \square

Remark. Results similar to Theorem 2.1 can be found in [21, §6] (see also the corrections in [22, §5]).

Remark. Let \mathcal{S} denote the coarse moduli space of supersingular genus-2 curves in characteristic 3. We have shown that the invariant I_C gives an isomorphism from \mathcal{S} to the affine line \mathbb{A}^1 .

3. SUPERSINGULAR GENUS-TWO CURVES AS TRIPLE COVERS OF ELLIPTIC CURVES.

In this section we classify all of the degree-3 maps $\varphi: C \rightarrow E$ over a given base field of characteristic 3, where C is a genus-2 curve and E is a supersingular elliptic curve. We start by writing down a family of such maps.

Let k be a field of characteristic 3, and let b and c be nonzero elements of k . Let $E_{b,c}$ be the elliptic curve

$$y^2 = x^3 - bx + c$$

and let $C_{b,c}$ be the genus-2 curve

$$w^2 = c(v^3 - bv^2 - b^2v + b^3 - c^2)(v^3 + bv^2 - b^2v - b^3 - c^2).$$

Lemma 3.1. *There are degree-3 maps*

$$\varphi_{b,c}: C_{b,c} \rightarrow E_{b,c} \quad \text{and} \quad \varphi'_{b,c}: C_{b,c} \rightarrow E_{-b,c}$$

that induce an isogeny $\text{Jac } C_{b,c} \rightarrow E_{b,c} \times E_{-b,c}$.

Proof. Let

$$\begin{aligned} x &= -bc(v-b)/(v^3 - bv^2 - b^2v + b^3 - c^2) \\ z &= -w/(v^3 - bv^2 - b^2v + b^3 - c^2) \\ y &= (z^3 + bxz)/c. \end{aligned}$$

One can check that then $y^2 = x^3 - bx + c$, so these equations define a degree-3 map $\varphi_{b,c}: C_{b,c} \rightarrow E_{b,c}$. Replacing b with $-b$ in the definition of $\varphi_{b,c}$ gives a degree-3 map $\varphi'_{b,c}: C_{b,c} \rightarrow E_{-b,c}$. It is an easy exercise to pull back the invariant differentials of $E_{b,c}$ and $E_{-b,c}$ to $C_{b,c}$ and to show that the pullbacks are linearly independent; it follows that the induced map $\text{Jac } C_{b,c} \rightarrow E_{b,c} \times E_{-b,c}$ is an isogeny. \square

Theorem 3.2. *Suppose C is a curve over a field k of characteristic 3, and suppose $\varphi: C \rightarrow E$ is a degree-3 map from C to a supersingular elliptic curve E over k . Then there exist nonzero $b, c \in k$ such that the cover $\varphi: C \rightarrow E$ is isomorphic $\varphi_{b,c}: C_{b,c} \rightarrow E_{b,c}$.*

Proof. The Riemann-Hurwitz formula shows that the degree of the different of φ is 2, so either there are two geometric points of C each contributing 1 to the different, or there is one geometric point contributing 2 to the different. A ramification analysis as in [7, §7.2] shows that no point can contribute 2 to the different; therefore, the triple cover φ must have exactly two ramification points P and Q , both tame.¹ Let $k(C)$ be the function field of C and let $k(E)$ be the function field of E . We can choose a generator z for $k(C)$ over $k(E)$ whose trace to $k(E)$ is 0; then z satisfies an equation $z^3 - fz = g$ for two functions f and g on E . From [7, §7.2] we see that f has odd order at a point of E if and only if that point contributes an odd amount to the different of φ ; therefore we must have

$$\text{div } f = P + Q + 2D - 2\infty$$

where D is a degree-0 divisor that is rational over k . We can write

$$D = -R + \infty + \text{div } r$$

for some function r and some point R on E , both rational over k . Replacing z with z/r , the function f with f/r^2 , and g with g/r^3 , we still have $z^3 - fz = g$, but now the divisor of f is $P + Q - 2R$. (Note that P and Q must be distinct because there

¹The analysis in [7, §7.2] assumes that the base field is finite and that the cover has been written in a certain standard form. However, for the ramification analysis all we need to know is that the cover can be put in the standard form locally everywhere, and this is true.

We should note that there is an error in [7, §7.2], starting at the second full paragraph on page 1717. The error is in the statement that either $2 \text{ord}_P g \geq 3 \text{ord}_P f$ or $\text{ord}_P g \not\equiv 0 \pmod{3}$, except when $P = \infty$ and $\text{ord}_P g = -3$. While this is true when $\text{ord}_P f = 0$, it can fail when $\text{ord}_P f = 1$. What is true is that for every $P \neq \infty$ for which $\text{ord}_P f > 0$, there is a constant $c_P \in \bar{k}$ such that either $2 \text{ord}_P(g + c_P^3 - c_P f) \geq 3 \text{ord}_P f$ or $\text{ord}_P(g + c_P^3 - c_P f) \not\equiv 0 \pmod{3}$. This change affects the statement in the final paragraph of [7, §7.2]. See [8] for more details.

are two ramification points, and R must be distinct from both P and Q , because otherwise the function f would have a single zero and a single pole.) Now we can change coördinates on E so that R is the point at infinity. After this change of coördinates, we have $P + Q = 0$ in the group law on E . Let the equation for E be $y^2 = x^3 - bx + c$, where $b \neq 0$. Then the function f must be of the form $f = d(x - a)$ for some $a \in k$ and $d \in k^*$. Shifting x by the constant a does not change the form of the equation for E , but now we may assume that $f = dx$ for some nonzero $d \in k$. Since P and Q are distinct and both are zeros of f , we see that $c \neq 0$.

We know from [7, §7] that by translating z by functions on E , we can modify g so that it only has poles at the poles of f ; thus we may assume that the only pole of g is at ∞ . Furthermore, using the statement from the first full paragraph on page 1717 of [7], we see that we can modify g so that it has at most a triple pole at ∞ . Therefore, we may assume that g is a linear combination of 1 , x , and y . By shifting z by an appropriate constant to eliminate the multiple of x appearing in this linear combination, we may assume that g is a linear combination of 1 and y .

Now we use the statement from the final paragraph of [7, §7.2], as corrected in the footnote above. We know that there are constants c_P and c_Q in \bar{k} such that

$$2 \operatorname{ord}_P(g + c_P^3 - c_P f) \geq 3 \operatorname{ord}_P f = 3$$

and

$$2 \operatorname{ord}_Q(g + c_Q^3 - c_Q f) \geq 3 \operatorname{ord}_Q f = 3.$$

The functions on the left-hand sides of these inequalities have degree at most 3, so their orders at P (and Q) are either 2 or 3. This means that the two lines

$$(1) \quad g + c_P^3 - c_P f = 0 \quad \text{and} \quad g + c_Q^3 - c_Q f = 0$$

must be the tangent lines to E at P and Q .

Let us write $P = (0, y_P)$ and $Q = (0, y_Q)$, with $y_Q = -y_P$. Then the tangent lines to E at P and Q are given by

$$(2) \quad y_P y - bx - y_P^2 = 0 \quad \text{and} \quad y_Q y - bx - y_Q^2 = 0$$

Note that the slopes of the lines defined by these two equations are negatives of one another, and the same is true of the y -intercepts of the two lines. Applying the first of these two observations to the lines defined in (1) shows that $c_Q = -c_P$. Applying the second observation then tells us that there can be no constant term appearing in the function g ; that is, $g = ey$ for some constant $e \in k$. Finally, by using this formula for g and the fact that the two pairs of lines (1) and (2) are equal, we find that we must have $b^3 e^2 + c^2 d^3 = 0$. Since b , c , and d are nonzero, so is e .

We have shown that the triple cover C of E can be written in the form

$$(3) \quad \begin{aligned} y^2 &= x^3 - bx + c \\ z^3 - dxz &= ey \end{aligned}$$

where b , c , d , and e are nonzero elements of k that satisfy $b^3 e^2 + c^2 d^3 = 0$. It is convenient to rescale the variables in these equations to get a more standardized form. Let r be a nonzero element of k , and replace z with rz , d with d/r^2 , and e with e/r^3 . Then the equations (3) still hold, but the ratio c/e has been replaced

with the ratio cr^3/e . If we choose $r = -(be)/(cd)$, then

$$\frac{cr^3}{e} = \frac{-cb^3e^3}{ec^3d^3} = \frac{-b^3e^2}{c^2d^3} = 1.$$

In other words, we may scale our variables so that $e = c$, from which it follows that $d = -b$.

We can find new equations defining C by setting

$$\begin{aligned} v &= -b + (z^2 - c)/x \\ w &= -z(v^3 - bv^2 - b^2v + b^3 - c^2). \end{aligned}$$

A straightforward computation then shows that v and w satisfy

$$w^2 = c(v^3 - bv^2 - b^2v + b^3 - c^2)(v^3 + bv^2 - b^2v - b^3 - c^2),$$

and that we have

$$\begin{aligned} x &= -bc(v - b)/(v^3 - bv^2 - b^2v + b^3 - c^2) \\ z &= -w/(v^3 - bv^2 - b^2v + b^3 - c^2) \\ y &= (z^3 + bxz)/c. \end{aligned}$$

This shows that any given genus-2 triple cover of a supersingular elliptic curve over a field k of characteristic 3 is isomorphic to a cover $\varphi_{b,c}: C_{b,c} \rightarrow E_{b,c}$ for some nonzero b and c in k . \square

Corollary 3.3. *If C is a genus-2 triple cover of a supersingular elliptic curve in characteristic 3, then C is supersingular.* \square

Note that if C is a triple cover of a supersingular elliptic curve, then the right-hand side of the equation for C factors into a product of two cubics. The converse is true as well.

Theorem 3.4. *Let C be a supersingular genus-2 curve over a field k of characteristic 3, and write C in the form $y^2 = f$ for a sextic polynomial f . If f can be written as the product of two cubic factors, then C is a triple cover of a supersingular elliptic curve.*

Proof. Neither the hypothesis nor the conclusion of the theorem depends on which model for C we choose, so we may replace the given f with any sextic that defines the same curve.

First we note that some quadratic twist of C can be written in the form $y^2 = f$, where

$$f = x^6 + Ax^3 + Bx + A^2$$

for some elements $A, B \in k$ with $B \neq 0$. For curves with $I_C \neq 0$ this follows from Theorem 2.2(c); for curves with $I_C = 0$ this follows from explicitly writing down the twists of the curve $y^2 = x^5 + 1$.

If we replace x in this equation with $-Bx$, and if we replace y with B^3y , we see that the new variables satisfy an equation of the same form as above, only now the new B has the property that $-B$ is a square.

Let g_1 and g_2 be monic cubics such that $f = g_1g_2$. Elementary manipulations show that the coefficients of x^2 in g_1 and g_2 are negatives of one another, and they

are both nonzero. Likewise, it is easy to show that the sum of the coefficients of x in g_1 and g_2 must be the square of the coefficient of x^2 . Thus we may write

$$\begin{aligned} g_1 &= x^3 + ux^2 + u^2vx + w \\ g_2 &= x^3 - ux^2 + u^2(1-v)x + t \end{aligned}$$

for some elements u, v, w, t of k with $u \neq 0$. Setting g_1g_2 equal to f , we find that we must have

$$t = w + u^3(v^2 - v)$$

and

$$w(v+1) = -u^3(v^4 - v^2 + 1).$$

The latter equality shows that $v \neq -1$.

For $i = 1, 2$ let h_i be g_i evaluated at $x + u(v+1)$. If we let c be a square root of $-B/u^2$ (which is possible because of the way we adjusted B at the beginning of the proof), then we have

$$\begin{aligned} h_1 &= x^3 + ux^2 - u^2x + u^3 - c^2 \\ h_2 &= x^3 - ux^2 - u^2x - u^3 - c^2. \end{aligned}$$

Thus some quadratic twist of our curve C is isomorphic to the curve $C_{u,c}$. But it is easy to see that a quadratic twist of a curve $C_{b,c}$ is isomorphic to a curve of the same form, so in any case, C is a triple cover of an elliptic curve. \square

Next we note that different (b, c) pairs can give rise to isomorphic covers $\varphi_{b,c}$.

Lemma 3.5. *Let b, c , and r be nonzero elements of k . Then the cover*

$$\varphi_{br^4, cr^6}: C_{br^4, cr^6} \rightarrow E_{br^4, cr^6}$$

is isomorphic to the cover $\varphi_{b,c}: C_{b,c} \rightarrow E_{b,c}$.

Proof. We can view the cover $\varphi_{b,c}: C_{b,c} \rightarrow E_{b,c}$ as being given by the equations (3), with $e = c$ and $d = -b$. If we let $X = r^2x$ and $Y = r^3y$ and $Z = r^3z$, then these equations become

$$\begin{aligned} Y^2 &= X^3 - br^4X + cr^6 \\ Z^3 + br^4XZ &= cr^6Y, \end{aligned}$$

which are the equations defining the cover

$$\varphi_{br^4, cr^6}: C_{br^4, cr^6} \rightarrow E_{br^4, cr^6}.$$

\square

Let \mathcal{A} denote the coarse moduli space of triples (C, E, φ) , where $\varphi: C \rightarrow E$ is a degree-3 map from a supersingular genus-2 curve in characteristic 3 to a supersingular elliptic curve. Let \mathcal{B} denote the coarse moduli space of pairs (C, G) , where C is a supersingular genus-2 curve in characteristic 3 and G is an order-4 subgroup of $(\text{Jac } C)[2]$ that is not isotropic with respect to the Weil pairing. There is a map $\kappa: \mathcal{A} \rightarrow \mathcal{B}$ that sends (C, E, φ) to $(C, (\ker \varphi_*)[2])$. Recall that \mathcal{S} denotes the coarse moduli space of supersingular genus-2 curves, and in Section 2 we gave an isomorphism $\mathcal{S} \rightarrow \mathbb{A}^1$.

Theorem 3.6. *Let notation be as above.*

- (1) The map $\kappa: \mathcal{A} \rightarrow \mathcal{B}$ is an isomorphism.
- (2) The function that sends a cover $\varphi_{b,c}$ to c^2/b^3 induces an isomorphism $\mathcal{A} \rightarrow \mathbb{A}^1 \setminus \{0\}$.
- (3) Under the isomorphisms $\mathcal{A} \rightarrow \mathbb{A}^1 \setminus \{0\}$ and $\mathcal{S} \rightarrow \mathbb{A}^1$ given above, the natural map $\mathcal{A} \rightarrow \mathcal{S}$ that sends (C, E, φ) to C is given by the function

$$t \mapsto -\frac{(1+t^4)^5}{t^{18}}.$$

Proof. If C is a genus-2 curve over a field of characteristic not 2, there are 35 geometric order-4 subgroups of $(\text{Jac } C)[2]$. Of these subgroups, there are 15 that are isotropic with respect to the Weil pairing. Therefore, the degree of the natural map $\mathcal{B} \rightarrow \mathcal{S}$ is 20.

Let \mathcal{C} denote $\mathbb{A}^1 \setminus \{0\}$, and let ι be the map from \mathcal{C} to \mathcal{A} that sends c to $C_{1,c}$. Lemma 3.5 shows that c and $-c$ have the same image in \mathcal{A} , so the degree of ι is at least 2. It is easy to compute that

$$(4) \quad I_{C_{1,c}} = -\frac{(1+c^8)^5}{c^{36}},$$

so the composition $\mathcal{C} \rightarrow \mathcal{A} \rightarrow \mathcal{S}$ has degree 40 and the map $\mathcal{A} \rightarrow \mathcal{S}$ has degree at most 20. But $\mathcal{A} \rightarrow \mathcal{S}$ factors through the degree-20 map $\mathcal{B} \rightarrow \mathcal{S}$, so we deduce that $\kappa: \mathcal{A} \rightarrow \mathcal{B}$ is an isomorphism and that ι has degree 2. In particular, this proves statement (1).

We also see that \mathcal{A} is isomorphic to the quotient of \mathcal{C} by $\{\pm 1\}$. This quotient is itself isomorphic to $\mathbb{A}^1 \setminus \{0\}$, and the isomorphism can be chosen so that the point on \mathcal{A} corresponding to $\varphi_{b,c}$ gets sent to the point c^2/b^3 of $\mathbb{A}^1 \setminus \{0\}$. This proves statement (2).

Statement (3) follows from equation (4). \square

Remark. Suppose C is a genus-2 curve defined by $y^2 = f$, where f is a degree-6 polynomial. Suppose g is a cubic factor of f . Then we can associate to g the subgroup of $(\text{Jac } C)[2]$ whose geometric points are the divisor classes that can be represented by divisors of the form $P - Q$, where P and Q are Weierstraß points whose x -coordinates are roots of g . The Weil pairing on two such divisors is given by the cardinality (modulo 2) of the intersection of their supports, so the subgroup associated to g is not isotropic. Since there are 20 cubic factors of f (over the algebraic closure) and 20 non-isotropic geometric order-4 subgroups of $(\text{Jac } C)[2]$, we can view the moduli space \mathcal{B} as the space of pairs (f, g) , where $y^2 = f$ is a supersingular genus-2 curve and g is a cubic factor of f .

4. SUPERSINGULAR ELLIPTIC CURVES OVER FINITE FIELDS OF CHARACTERISTIC THREE

In this section we list the different isomorphism classes of supersingular elliptic curves over finite fields of characteristic 3. We specify how the different isomorphism classes are Galois twists of one another, and we compute their traces of Frobenius. This information will enable us to compute the Weil polynomials of supersingular genus-2 curves in Section 5.

Let E be the elliptic curve $y^2 = x^3 - x$ over \mathbb{F}_3 . For every finite extension \mathbb{F}_q of \mathbb{F}_3 , we will express all the isomorphism classes of supersingular elliptic curves over \mathbb{F}_q as twists of E .

Condition on b	Condition on c	# Aut E'	Cohomology class	Trace
$\chi_{q,2}(b) = 1$	$\text{Tr } c/s(b)^3 = 0$	6	$\{\pm 1\}$	0
$\chi_{q,2}(b) = 1$	$\text{Tr } c/s(b)^3 = 1$	6	$\{\omega, -\omega^2\}$	$(-3)^{(d+1)/2}$
$\chi_{q,2}(b) = 1$	$\text{Tr } c/s(b)^3 = 2$	6	$\{-\omega, \omega^2\}$	$-(-3)^{(d+1)/2}$
$\chi_{q,2}(b) = -1$	(no condition)	2	$\{\pm \iota, \pm \iota\omega, \pm \iota\omega^2\}$	0

TABLE 1. The twists $E': y^2 = x^3 - bx + c$ of the elliptic curve $y^2 = x^3 - x$ over \mathbb{F}_{3^d} , when d is odd.

Let $i \in \mathbb{F}_9$ be a square root of -1 . Let ι, ω , and π be the following endomorphisms of $E_{\mathbb{F}_9}$:

$$\begin{aligned}\iota &: (x, y) \mapsto (-x, iy) \\ \omega &: (x, y) \mapsto (x - 1, y) \\ \pi &: (x, y) \mapsto (x^3, y^3).\end{aligned}$$

One can check that the following relations hold in $\text{End } E_{\mathbb{F}_9}$:

$$\iota\omega = \omega^2\iota, \quad \iota\pi = -\pi\iota, \quad \omega\pi = \pi\omega, \quad \pi = 1 + 2\omega.$$

The automorphism group A of $E_{\mathbb{F}_3}$ is the group of order 12 generated by ι and ω .

Let $q = 3^d$ be a power of 3. The twists of $E_{\mathbb{F}_q}$ are catalogued by the pointed cohomology set $H^1(\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q), A)$. We identify a cocycle $\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \rightarrow A$ with the image of the q -power Frobenius automorphism in A ; using this identification, we view a cohomology class as a set of elements of A . We let the reader verify that when d is odd (so that the Galois action on A is nontrivial) we have

$$H^1(\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q), A) = \{\{\pm 1\}, \{\omega, -\omega^2\}, \{-\omega, \omega^2\}, \{\pm \iota, \pm \iota\omega, \pm \iota\omega^2\}\},$$

and when d is even (so the Galois action on A is trivial) we have

$$\begin{aligned}H^1(\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q), A) = \\ \{\{1\}, \{-1\}, \{\omega, \omega^2\}, \{-\omega, -\omega^2\}, \{\iota, \iota\omega, \iota\omega^2\}, \{-\iota, -\iota\omega, -\iota\omega^2\}\}.\end{aligned}$$

Every supersingular elliptic curve E' over \mathbb{F}_q can be written in the form $y^2 = x^3 - bx + c$ with $b \neq 0$, and every curve of this form is supersingular. In Table 1 we enumerate the isomorphism classes of the twists of E in the case that d is odd, and we show how one can determine the cohomology class corresponding to a supersingular elliptic curve E' from the coefficients b and c of its defining equation. The verification of the table is a straightforward exercise; we simply note that the Frobenius endomorphism of the twist of E by the cohomology class containing an automorphism ζ can be taken to be $\zeta\pi^d$, where π is the \mathbb{F}_3 -Frobenius of E (as above). The table refers to the quadratic character $\chi_{q,2}: \mathbb{F}_q^* \rightarrow \{\pm 1\}$ defined by $\chi_{q,2}(x) = x^{(q-1)/2}$ and to the absolute trace function $\text{Tr}: \mathbb{F}_q \rightarrow \mathbb{F}_3$. The table also uses the notation $s(b)$ to denote the quantity $b^{(3-q)/4}$; since $q \equiv 3 \pmod{8}$, we see that $s(b)$ is always a square, and when b is a square, $s(b)$ is the unique square root of b that is itself a square.

In Table 2 we enumerate the isomorphism classes of the twists of E in the case that d is even. The table refers to the quartic character $\chi_{q,4}: \mathbb{F}_q^* \rightarrow \{\pm 1, \pm i\}$

Condition on b	Condition on c	# Aut E'	Cohomology class	Trace
$\chi_{q,4}(b) = 1$	$\text{Tr } c/b^{3/2} = 0$	12	$\{1\}$	$2(-3)^{d/2}$
	$\text{Tr } c/b^{3/2} \neq 0$	6	$\{\omega, \omega^2\}$	$-(-3)^{d/2}$
$\chi_{q,4}(b) = -1$	$\text{Tr } c/b^{3/2} = 0$	12	$\{-1\}$	$-2(-3)^{d/2}$
	$\text{Tr } c/b^{3/2} \neq 0$	6	$\{-\omega, -\omega^2\}$	$(-3)^{d/2}$
$\chi_{q,4}(b) = i$	(no condition)	4	$\{-\iota, -\iota\omega, -\iota\omega^2\}$	0
$\chi_{q,4}(b) = -i$	(no condition)	4	$\{\iota, \iota\omega, \iota\omega^2\}$	0

TABLE 2. The twists $E': y^2 = x^3 - bx + c$ of the elliptic curve $y^2 = x^3 - x$ over \mathbb{F}_{3^d} , when d is even.

defined by $\chi_{q,2}(x) = x^{(q-1)/4}$ and to the absolute trace function $\text{Tr}: \mathbb{F}_q \rightarrow \mathbb{F}_3$. The conditions that involve $b^{3/2}$ do not depend on the choice of the square root of b .

5. WEIL POLYNOMIALS OF SUPERSINGULAR GENUS-TWO CURVES IN CHARACTERISTIC THREE

In this section we determine the polynomials that occur as Weil polynomials of supersingular genus-2 curves over finite fields of characteristic 3. In fact, for every polynomial that occurs as the Weil polynomial of a supersingular genus-2 curve over \mathbb{F}_q , we show how to quickly construct an explicit curve with this Weil polynomial.

To begin, let us record for convenience a list of the Weil polynomials of supersingular abelian surfaces over the finite fields of characteristic 3.

Lemma 5.1. *Let $q = 3^d$ be a power of 3. If d is odd, then the polynomials that occur as the Weil polynomials of supersingular abelian surfaces over \mathbb{F}_q are:*

- (1) $(x^2 - sx + q)(x^2 - tx + q)$ for all $s, t \in \{0, \pm\sqrt{3q}\}$;
- (2) $x^4 + q^2$;
- (3) $x^4 + qx^2 + q^2$;
- (4) $x^4 - 2qx^2 + q^2$.

If d is even, the polynomials that occur as the Weil polynomials of supersingular abelian surfaces over \mathbb{F}_q are:

- (1) $(x^2 - sx + q)(x^2 - tx + q)$ for all $s, t \in \{0, \pm\sqrt{q}, \pm 2\sqrt{q}\}$;
- (2) $x^4 + q^2$;
- (3) $x^4 - qx^2 + q^2$;
- (4) $x^4 - sx^3 + qx^2 - sqx + q^2$ for all $s \in \{\pm\sqrt{q}\}$.

Proof. We already know the Weil polynomials of the supersingular elliptic curves over \mathbb{F}_q , and on each of the lists in the lemma, item (1) gives the Weil polynomials of the products of these curves. The remaining polynomials on each list correspond to simple abelian surfaces; this follows from [14, Cor. 2.8, Thm. 2.9]. The cited results also show that the lists are complete. \square

To prove Theorem 1.1, then, we must go through the lists in Lemma 5.1 and determine which entries come from genus-2 curves.

Proof of Theorem 1.1. We begin with the case when the degree of \mathbb{F}_q over \mathbb{F}_3 is even. The result when $q = 9$ can be obtained by direct computation, so we will

Condition on b	Condition on c	s	t
$\chi_{q,4}(b) = 1$	$\text{Tr}_{\mathbb{F}_q/\mathbb{F}_9} c/b^{3/2} = 0$	$2(-3)^{d/2}$	$2(-3)^{d/2}$
	$\text{Tr}_{\mathbb{F}_q/\mathbb{F}_9} c/b^{3/2} = \pm 1 \pm i$	$-(-3)^{d/2}$	$-(-3)^{d/2}$
	$\text{Tr}_{\mathbb{F}_q/\mathbb{F}_9} c/b^{3/2} \in \{\pm 1, \pm i\}$	$2(-3)^{d/2}$	$-(-3)^{d/2}$
$\chi_{q,4}(b) = -1$	$\text{Tr}_{\mathbb{F}_q/\mathbb{F}_9} c/b^{3/2} = 0$	$-2(-3)^{d/2}$	$-2(-3)^{d/2}$
	$\text{Tr}_{\mathbb{F}_q/\mathbb{F}_9} c/b^{3/2} = \pm 1 \pm i$	$(-3)^{d/2}$	$(-3)^{d/2}$
	$\text{Tr}_{\mathbb{F}_q/\mathbb{F}_9} c/b^{3/2} \in \{\pm 1, \pm i\}$	$-2(-3)^{d/2}$	$(-3)^{d/2}$
$\chi_{q,4}(b) = \pm i$	(no condition)	0	0

TABLE 3. The conditions on b and c that determine the Weil polynomial $(x^2 - sx + q)(x^2 - tx + q)$ of the curve $C_{b,c}$, when $q = 3^d$ and d is even. The function $\chi_{q,4}$ is the character defined in Section 3.

assume that $q > 9$. We begin by providing, for every Weil polynomial in the second list in Theorem 1.1, a curve with that Weil polynomial.

Items (1), (2), and (3): The split polynomials. For each of the polynomials listed in items (1), (2), and (3) we can find a curve $C_{b,c}$ with that Weil polynomial. This is clear from Table 3, in which we give simple conditions on b and c that determine the Weil polynomial of the curve $C_{b,c}$. It is easy to use Lemma 3.1 and Table 2 to verify that the entries of Table 3 are correct.

Item (4): The polynomial $x^4 + q^2$. Let $a \in \mathbb{F}_q$ be a nonsquare, and let C be the curve

$$y^2 = z^6 + z^3 + az + a^3 + 1$$

over \mathbb{F}_q . Over \mathbb{F}_{q^2} we can write C as

$$y^2 = (z^3 - \sqrt{-a}z^2 + az - a\sqrt{-a} - 1)(z^3 + \sqrt{-a}z^2 + az + a\sqrt{-a} - 1)$$

so that $C_{\mathbb{F}_{q^2}}$ is isomorphic to $C_{\sqrt{-a},1}$. It is easy to check that the isogeny

$$\text{Jac } C_{\mathbb{F}_{q^2}} \rightarrow E_{\sqrt{-a},1} \times E_{-\sqrt{-a},1}$$

from Lemma 3.1 descends to give an isogeny from $\text{Jac } C$ to the restriction of scalars of $E_{\sqrt{-a},1}$. We see from Table 2 that the Weil polynomial of $E_{\sqrt{-a},1}$ is $x^2 + q^2$ (because the square root of a nonsquare in \mathbb{F}_q is a nonsquare in \mathbb{F}_{q^2} , when q is a power of 9, because the group $\mathbb{F}_{q^2}^*/\mathbb{F}_q^*$ has order 2 mod 4), so the Weil polynomial for C is $x^4 + q^2$.

Item (5): The polynomials $x^4 - sx^3 + qx^2 - sqx + q^2$, where $s^2 = q$. Let $f = x^4 - sx^3 + qx^2 - sqx + q^2$, where s is a square root of q . The main result of [9] shows that the isogeny class of abelian surfaces corresponding to f contains a principally polarized variety A . We see from [14, Table 1, p. 325] that the simple variety A remains simple over \mathbb{F}_{q^2} , and [14, Thm. 4.1] then shows that A is the Jacobian of a curve over \mathbb{F}_q .

(One can also construct explicit curves with these Weil polynomials as follows. Note that the map $\mathbb{F}_q \rightarrow \mathbb{F}_q$ given by $z \mapsto z^5 - z^2$ is not surjective, because 0 and 1 both get sent to 0. Therefore there is a nonzero $c \in \mathbb{F}_q$ such that the polynomial $g = z^5 - z^2 - c$ has no roots in \mathbb{F}_q . The discriminant of g is $-c^4$, which is a square in \mathbb{F}_q , so a result of Pellet [17] shows that g has an even number of irreducible factors

s	t	S	T
$-2(-3)^{d/2}$	$-(-3)^{d/2}$	$2q^d$	$-q^d$
$-(-3)^{d/2}$	0	$-q^d$	$-2q^d$
0	$(-3)^{d/2}$	$-2q^d$	$-q^d$
$(-3)^{d/2}$	$2(-3)^{d/2}$	$-q^d$	$2q^d$
$-2(-3)^{d/2}$	0	$2q^d$	$-2q^d$
0	$2(-3)^{d/2}$	$-2q^d$	$2q^d$
$-(-3)^{d/2}$	$(-3)^{d/2}$	$-q^d$	$-q^d$
$-2(-3)^{d/2}$	$2(-3)^{d/2}$	$2q^d$	$2q^d$

TABLE 4. Certain split Weil polynomials $(x^2 - sx + q)(x^2 - tx + q)$ over \mathbb{F}_q , and the corresponding Weil polynomials $(x^2 - Sx + q)(x^2 - Tx + q)$ over \mathbb{F}_{q^2} . Here $q = 3^d$ for an even number d .

of even degree. Since g has no linear factors, it follows that g is irreducible. Then \mathbb{F}_{q^5} is the smallest extension of \mathbb{F}_q over which the Jacobian of the supersingular curve $C: y^2 = z(z^5 - z^2 - c)$ has rational 2-torsion points, so the Weil polynomial of C is not any of the polynomials listed in items (1) through (3) of the second list in Lemma 5.1. The only possibility remaining is that C and its quadratic twist give us the two Weil polynomials $x^4 - sx^3 + qx^2 - sqx + q^2$, where $s^2 = q$.)

Of the polynomials given in the second list of Lemma 5.1, we have shown that those that appear in the second list of Theorem 1.1 do occur as the Weil polynomials of Jacobians; now we must show that the remaining polynomials from the second list of Lemma 5.1 do not come from Jacobians. We begin with the split isogeny classes.

In Table 4 we list the split Weil polynomials over \mathbb{F}_q that we must show do not occur. Suppose C is a curve over \mathbb{F}_q with one of these Weil polynomials. Write C as $y^2 = f$ for some sextic polynomial $f \in \mathbb{F}_q[z]$. If f has a cubic factor, then Theorems 3.4 and 3.2, together with Lemma 3.1 and Table 2, show that the Weil polynomial for C cannot factor in the way we have assumed. (The key fact to notice is that the quartic character $\chi_{q,4}$ takes the same value on b and on $-b$.) Therefore, the polynomial f is either

- an irreducible sextic;
- the product of a linear polynomial with an irreducible quintic;
- the product of a quadratic polynomial with an irreducible quartic; or
- the product of three irreducible quadratics.

Corresponding to these factorizations of f , we obtain information about the reduction of the Weil polynomial of C modulo 2. In the four cases listed above, the Weil polynomial modulo 2 is

- $(x^2 + x + 1)^2$;
- $(x^4 + x^3 + x^2 + x + 1)$;
- $(x + 1)^4$; and
- $(x + 1)^4$.

Note that the first four Weil polynomials in Table 4 do not factor modulo 2 in any of these ways, so these first four polynomials do not occur as the Weil polynomials of Jacobians over \mathbb{F}_q .

For the next two entries in the table, we notice that the corresponding Weil polynomials over \mathbb{F}_{q^2} are both $(x^2 - 2qx + q^2)(x^2 + 2qx + q^2)$. We see that f is therefore not the product of a linear polynomial and an irreducible quintic. Looking at the other possible factorizations of f over \mathbb{F}_q , we see that f must have a cubic factor over \mathbb{F}_{q^2} . Once again, Theorem 3.4, Theorem 3.2, Lemma 3.1, and Table 2 show that this Weil polynomial over \mathbb{F}_{q^2} cannot occur.

For the penultimate entry in Table 4, we again use Theorem 3.4, Theorem 3.2, Lemma 3.1, and Table 2. We find that over \mathbb{F}_{q^2} , our hypothetical curve C must be isomorphic to $C_{b,c}$ for some $b, c \in \mathbb{F}_{q^2}$ where b is a fourth power and where the absolute traces of $c/b^{3/2}$ and of $c/(-b)^{3/2}$ are both nonzero. Using Lemma 3.5, we can assume that $b = 1$, so that $c \in \mathbb{F}_{q^2}$ now has the property that c and ic have nonzero trace to \mathbb{F}_3 . It must certainly be the case that c has nonzero trace to \mathbb{F}_9 . Now, we know from equation (4) and from the fact that C is defined over \mathbb{F}_q that we must have

$$\frac{(c^8 + 1)^5}{c^{36}} \in \mathbb{F}_q.$$

Applying Lemma 5.2 (below) with $r = 9$, we find that c must actually lie in \mathbb{F}_q . From this it follows that C is a twist of the curve $C_{1,c}$ over \mathbb{F}_q . But again using Lemma 3.1 and Table 2, we see that $C_{1,c}$ has Weil polynomial $(x^2 + 3^{d/2}x + q)^2$, so the Weil polynomial of C must be either $(x^2 + 3^{d/2}x + q)^2$ or $(x^2 - 3^{d/2}x + q)^2$. This contradicts our assumption that C has Weil polynomial $(x^2 + 3^{d/2}x + q)(x^2 - 3^{d/2}x + q)$.

We turn to the final entry in Table 4. Write our hypothetical curve C as $dy^2 = f$ for some nonzero d in \mathbb{F}_q and some degree-6 polynomial f . From what we have already noted, we know that f is either the product of three irreducible quadratics, or is the product of an irreducible quartic with a quadratic. In either case f has a cubic factor over \mathbb{F}_{q^2} . Theorem 3.4, Theorem 3.2, Lemma 3.1, and Table 2 show that $C_{\mathbb{F}_{q^2}}$ is isomorphic to $C_{b,c}$ for some $b, c \in \mathbb{F}_{q^2}^*$, where b is a fourth power and where the trace of $c/b^{3/2}$ from \mathbb{F}_{q^2} to \mathbb{F}_9 is equal to 0. Without loss of generality, we may assume that $b = 1$. Equation (4) shows that $(1 + c^8)^5/c^{36}$ lies in \mathbb{F}_{q^2} (indeed, it lies in \mathbb{F}_q), and applying Lemma 5.3 (below) with $r = 9$ and $Q = q^2$ shows that all of the geometric points of \mathcal{A} lying above the point P_C of \mathcal{S} corresponding to C are rational over \mathbb{F}_{q^2} . Therefore all of the geometric points of \mathcal{B} lying above P_C are rational over \mathbb{F}_{q^2} , and it follows that all of the geometric cubic factors of f are rational over \mathbb{F}_{q^2} ; in other words, f splits completely over \mathbb{F}_{q^2} . Hence we see that f must be the product of three irreducible quadratics over \mathbb{F}_q .

At the beginning of the proof of Theorem 2.1 we showed that every supersingular genus-2 curve over \mathbb{F}_q can be written in the form $dy^2 = z^6 + c_3z^3 + c_1z + c_0$, so we may assume that our polynomial f has the form of the right-hand side of this equation. Then the discriminant of f is $-c_1^6$, and since \mathbb{F}_q is an even-degree extension of \mathbb{F}_3 , the discriminant is a square. But a polynomial over a finite field with a square discriminant has an even number of irreducible even-degree factors [17], so f cannot be the product of three irreducible quadratics. This contradiction shows that there is no supersingular curve over \mathbb{F}_q whose Weil polynomial is given by the final entry in Table 4.

Finally, we must show that there is no supersingular genus-2 curve with Weil polynomial $x^4 - qx^2 + q^2$. If there were such a curve C over \mathbb{F}_q , then reasoning as above shows that C must be given by an equation $y^2 = (\text{sextic})$, which shows that $C_{\mathbb{F}_{q^2}}$ has a degree-3 map to an elliptic curve. In fact, since the quadratic twist D of $C_{\mathbb{F}_{q^2}}$ has Weil polynomial $(x^2 + qx + q^2)^2$, we find from Table 3 that D is isomorphic to $C_{1,c}$ for some $c \in \mathbb{F}_{q^2}$ whose trace to \mathbb{F}_9 is $\pm 1 \pm i$. But since D is a twist of a curve over \mathbb{F}_q , we know that

$$I_D = -\frac{(c^8 + 1)^5}{c^{36}}$$

is an element of \mathbb{F}_q . Then Lemma 5.2 shows that c must be an element of \mathbb{F}_q , so our original curve C is a twist of a curve $C_{1,c}$. But $C_{1,c}$ has a split Jacobian and C does not, and this contradiction shows that there is no curve over \mathbb{F}_q with Weil polynomial $x^4 - qx^2 + q^2$.

This completes the proof of Theorem 1.1 in the case that d is even. We now turn to the case in which d is odd. The results when $q = 3$ can be obtained by enumerating all of the supersingular genus-2 curves over \mathbb{F}_3 and computing their Weil polynomials, so we will assume that $q > 3$.

Let us begin by giving examples of curves whose Weil polynomials comprise all the polynomials given in the first list of Theorem 1.1.

Items (1) and (2): The split polynomials. Let c_0, c_1 , and c_2 be nonzero elements of \mathbb{F}_q whose traces to \mathbb{F}_3 are 0, 1, and 2, respectively. Using Lemma 3.1 and Table 1, it is easy to check that the curve C_{1,c_1} has Weil polynomial

$$(x^2 + q)(x^2 - (-1)^{(d+1)/2} \sqrt{3qx + q}),$$

that the curve C_{1,c_2} has Weil polynomial

$$(x^2 + q)(x^2 + (-1)^{(d+1)/2} \sqrt{3qx + q}),$$

and that the curve C_{1,c_0} has Weil polynomial

$$(x^2 + q)^2.$$

Item (3): The polynomial $x^4 + q^2$. We calculate that the supersingular curve $y^2 = z^5 + 1$ over \mathbb{F}_3 has Weil polynomial $x^4 + 9$. It follows that the Weil polynomial for this curve over \mathbb{F}_q is $x^4 + q^2$ whenever q is an odd power of 3.

Item (4): The polynomial $x^4 + qx^2 + q^2$. Let a be an element of \mathbb{F}_q whose absolute trace is nonzero. Let $i \in \mathbb{F}_9$ be a square root of -1 , let b be the element ia^2 of \mathbb{F}_{q^2} , and let $c = -a^4$. Let C be the curve

$$y^2 = -a^4(z^6 + a^8 z^3 + a^{12} z + a^{16} + a^{12})$$

over \mathbb{F}_q . Note that over \mathbb{F}_{q^2} we have

$$z^6 + a^8 z^3 + a^{12} z + a^{16} + a^{12} = (z^3 - ia^2 z^2 + a^4 z - ia^6 - a^8)(z^3 + ia^2 z^2 + a^4 z + ia^6 - a^8)$$

so that $C_{\mathbb{F}_{q^2}} \cong C_{b,c}$. If we identify $C_{b,c}$ with $C_{\mathbb{F}_{q^2}}$ in the obvious way then the Galois group of \mathbb{F}_{q^2} over \mathbb{F}_q interchanges the two morphisms $\varphi_{b,c}: C \rightarrow E_{b,c}$ and $\varphi'_{b,c}: C \rightarrow E_{-b,c}$. It follows that the isogeny

$$\text{Jac } C_{\mathbb{F}_{q^2}} \rightarrow E_{b,c} \times E_{-b,c}$$

over \mathbb{F}_{q^2} descends to give an isogeny

$$\text{Jac } C \rightarrow \text{Res}_{\mathbb{F}_{q^2}/\mathbb{F}_q} E_{b,c}$$

from the Jacobian of C to the restriction of scalars of $E_{b,c}$. Since i is a square but not a fourth power in \mathbb{F}_9 , it is easy to see that $\chi_{q^2,4}(ia^2) = -1$. It is also easy to check that

$$\begin{aligned} \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_3} c/b^{3/2} &= \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_3} (1-i)a = \mathrm{Tr}_{\mathbb{F}_9/\mathbb{F}_3} \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_9} (1-i)a \\ &= \mathrm{Tr}_{\mathbb{F}_9/\mathbb{F}_3} (1-i) \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_9} a = \mathrm{Tr}_{\mathbb{F}_9/\mathbb{F}_3} (1-i) \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_3} a \\ &= -\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_3} a \neq 0, \end{aligned}$$

so by Table 2 we see that the Weil polynomial for $E_{b,c}$ is $x^2 + qx + q^2$. It follows that the Weil polynomial for $\mathrm{Res}_{\mathbb{F}_{q^2}/\mathbb{F}_q} E_{b,c}$ is $x^4 + qx^2 + q^2$, so $\mathrm{Jac} C$ has this Weil polynomial as well.

(Note that the quadratic twist of this C also has Weil polynomials $x^4 + qx^2 + q^2$. By rescaling the variables in the equation for the twist, we find that

$$y^2 = z^6 + a^2 z^3 + a^2 z + a^4 + 1$$

has Weil polynomial $x^4 + qx^2 + q^2$ whenever a is an element of \mathbb{F}_q whose absolute trace is nonzero.)

Item (5): The polynomial $x^4 - 2qx^2 + q^2$. We use a similar construction to produce a curve with Weil polynomial $x^4 - 2qx^2 + q^2$. Let $a \in \mathbb{F}_q$ be a nonzero element whose absolute trace is 0, let $i \in \mathbb{F}_9$ be as above, and again take $b = ia^2 \in \mathbb{F}_{q^2}$ and $c = -a^4$. We again find that the curve C over \mathbb{F}_q defined by

$$y^2 = z^6 + a^2 z^3 + a^2 z + a^4 + 1$$

has Jacobian isogenous to the restriction of scalars of $E_{b,c}$, but now Table 2 shows that the Weil polynomial of $E_{b,c}$ is $x^2 - 2qx + q^2$. It follows that the Weil polynomial of C is $x^4 - 2qx^2 + q^2$.

To complete the proof of Theorem 1.1, we must show that no curve over \mathbb{F}_q has Weil polynomial

$$(x^2 - \varepsilon_1 \sqrt{3q} + q)(x^2 - \varepsilon_2 \sqrt{3q} + q)$$

for any choice of $\varepsilon_1, \varepsilon_2 \in \{1, -1\}$. Suppose, to obtain a contradiction, that C is a curve over \mathbb{F}_q with such a Weil polynomial. Write C as $y^2 = f$ for a degree-6 polynomial $f \in \mathbb{F}_q[z]$. Note that f is not the product of a linear polynomial with an irreducible quintic, because if this were the case the minimal polynomial of Frobenius on the 2-torsion of C would be $x^4 + x^3 + x^2 + x + 1$. By enumerating the other possible factorization for f , we see that over \mathbb{F}_{q^2} , the polynomial f can be written a product of two (not-necessarily-irreducible) cubics. Therefore, by Theorems 3.4 and 3.2, $C_{\mathbb{F}_{q^2}}$ is isomorphic to $C_{b,c}$ for some $b, c \in \mathbb{F}_{q^2}^*$.

A simple computation shows that the Weil polynomial for $C_{\mathbb{F}_{q^2}}$ is

$$(x^2 - qx + q^2)^2,$$

so Lemma 3.1 and Table 2 show that $\chi_{q^2,4}(b) = \chi_{q^2,4}(-b) = 1$ and that the traces of $c/b^{3/2}$ and of $c/(-b)^{3/2}$ from \mathbb{F}_{q^2} to \mathbb{F}_3 are nonzero. Using Lemma 3.5, we can assume without loss of generality that $b = 1$. Then we know that $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_3} c \neq 0$, and in particular $\mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_9} c$ is nonzero.

Equation (4) tells us that

$$I_C = -\frac{(c^8 + 1)^5}{c^{36}}.$$

In particular, we note that $I_C \neq 0$, because the roots of $z^8 + 1$ generate \mathbb{F}_{81} , and \mathbb{F}_{q^2} is not an extension of \mathbb{F}_{81} . It follows from Theorem 2.2(c) that the geometric automorphism group of C has order 2. We also know that I_C is an element of \mathbb{F}_q , because C is a curve over \mathbb{F}_q .

Using Lemma 5.4 (below), we see that there is an element $\bar{c} \in \mathbb{F}_q$ such that

$$-\frac{(\bar{c}^8 + 1)^5}{\bar{c}^{36}} = \pm I_C.$$

If the equality holds with the plus sign, take $\bar{b} = 1$; if it holds with the minus sign, take $\bar{b} = i$, where i is a square root of -1 in \mathbb{F}_9 . Then we have $I_{C_{\bar{b}, \bar{c}}} = I_C$.

We claim that there is a curve D over \mathbb{F}_q such that $D_{\mathbb{F}_{q^2}} \cong C_{\bar{b}, \bar{c}}$. If $\bar{b} = 1$ then this is obvious. If $\bar{b} = i$, then we note that $C_{\bar{b}, \bar{c}}$ is defined by the equation

$$\begin{aligned} y^2 &= \bar{c}(z^3 - iz^2 + z - i - \bar{c}^2)(z^3 + iz^2 + z + i - \bar{c}^2) \\ &= \bar{c}(z^6 + \bar{c}^2 z^3 + \bar{c}^2 z + \bar{c}^4 + 1), \end{aligned}$$

so we can take D to be the curve over \mathbb{F}_q defined by this equation.

The fact that $I_D = I_C$ shows that D is a twist of C ; since the geometric automorphism group of C has order 2 the only nontrivial twist of C is the standard quadratic twist. This shows that the Weil polynomial of the curve D is of the form

$$(5) \quad (x^2 - \bar{\varepsilon}_1 \sqrt{3q} + q)(x^2 - \bar{\varepsilon}_2 \sqrt{3q} + q)$$

for some $\bar{\varepsilon}_1, \bar{\varepsilon}_2 \in \{1, -1\}$, and the Weil polynomial of $D_{\mathbb{F}_{q^2}}$ is

$$(6) \quad (x^2 - qx + q^2)^2.$$

If $\bar{b} = 1$, then we see from Lemma 3.1 and Table 1 that the Weil polynomial of D cannot be of the form given by (5). If $\bar{b} = i$, then we note that $\chi_{q^2, 4}(i) = -1$, so that Lemma 3.1 and Table 2 show that the Weil polynomial of $D_{\mathbb{F}_{q^2}}$ cannot be of the form given by (6). These contradictions shows that there can be no curve C over \mathbb{F}_q with Weil polynomial

$$(x^2 - \varepsilon_1 \sqrt{3q} + q)(x^2 - \varepsilon_2 \sqrt{3q} + q)$$

for any choice of $\varepsilon_1, \varepsilon_2 \in \{1, -1\}$. \square

We end by proving the three lemmas that we needed in the preceding proof.

Lemma 5.2. *Let r be a power of an odd prime p , and let q be a power of r . If $c \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ satisfies $(c^{r-1} + 1)^{(r+1)/2} / c^{r(r-1)/2} \in \mathbb{F}_q$, then $\text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_r} c = 0$.*

Proof. Let $G = \text{PSL}_2(\mathbb{F}_r)$, and consider the rational function

$$F = \frac{((z^r - z)^{r-1} + 1)^{(r+1)/2}}{(z^r - z)^{r(r-1)/2}} = \frac{(z^{r^2} - z)^{(r+1)/2}}{(z^r - z)^{(r^2+1)/2}}.$$

It is easy to verify that F is fixed by the action of G on $\mathbb{F}_r(z)$ by fractional linear transformations. Since the degree of F is equal to $\#G$, we know that for every $z_0 \in \mathbb{F}_r$, the roots of $F(z) - F(z_0)$ in \mathbb{F}_r are precisely the images of z_0 under the action of G . Furthermore, if $F(z_0)$ is nonzero then one can verify that

$$((z^r - z)^{r-1} + 1)^{(r+1)/2} - F(z_0)(z^r - z)^{r(r-1)/2}$$

is a separable polynomial, so G acts faithfully on the roots of $F(z) - F(z_0)$.

Let c be as in the statement of the lemma. Suppose that the trace of c to \mathbb{F}_r were not 0. Then the polynomial $z^r - z - c$ would have no roots in \mathbb{F}_{q^2} , so all of the roots of $z^r - z - c$ live in an extension of \mathbb{F}_{q^2} of degree divisible by p . Let d be such a root, and let $n = [\mathbb{F}_q(d) : \mathbb{F}_q]$, so that n is a multiple of $2p$. Then the hypothesis of the first statement of the lemma is that $F(d) \in \mathbb{F}_q$.

Since d^q is another root of $F(z) - F(d)$, we know there is an element σ of $\text{PSL}_2(\mathbb{F}_r)$ so that $d^q = \sigma(d)$. The element σ of G is fixed by the action of the absolute Galois group of \mathbb{F}_q , so we find that $d^{q^i} = \sigma^i(d)$ for all integers $i \geq 0$. Thus σ^n is the smallest power of σ that fixes d . In particular, the order of σ is a multiple of $2p$. But there are no elements of order $2p$ in G , because there are no involutions in G that commute with a nontrivial translation. This contradiction proves the lemma. \square

Lemma 5.3. *Let r be a power of an odd prime p , and let Q be a power of r . Suppose $c \in \mathbb{F}_Q$ satisfies $\text{Tr}_{\mathbb{F}_Q/\mathbb{F}_r} c = 0$, and let $e = (c^{r-1} + 1)^{(r+1)/2} / c^{r(r-1)/2}$. Then the polynomial*

$$(z^{r-1} + 1)^{(r+1)/2} - ez^{r(r-1)/2}$$

splits completely over \mathbb{F}_Q .

Proof. Since $\text{Tr}_{\mathbb{F}_Q/\mathbb{F}_r} c = 0$, there is a $d \in \mathbb{F}_Q$ with $c = d^r - d$. Let F be as in the preceding proof. Then all of the zeroes of the function $F(z) - F(d) = F(z) - e$ lie in \mathbb{F}_Q , and it follows that the polynomial in the statement of the lemma splits completely. \square

Lemma 5.4. *Let q be an odd power of 3. Suppose $c \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ satisfies $(c^8 + 1)^5 / c^{36} \in \mathbb{F}_q$ and that $\text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_9}(c)$ is nonzero. Then there is a $\bar{c} \in \mathbb{F}_q$ such that*

$$\frac{(\bar{c}^8 + 1)^5}{\bar{c}^{36}} = \pm \frac{(c^8 + 1)^5}{c^{36}}.$$

Proof. We use many of the ideas from the proof of Lemma 5.2. Let $G = \text{PSL}_2(\mathbb{F}_9)$ and let F be the rational function

$$F = \frac{((z^9 - z)^8 + 1)^5}{(z^9 - z)^{36}} = \frac{(z^{81} - z)^5}{(z^9 - z)^{41}}.$$

Since the trace of c to \mathbb{F}_9 is nonzero, we know that the polynomial $z^9 - z - c$ over \mathbb{F}_{q^2} factors as a product of cubics. Let d be an element of $\overline{\mathbb{F}}_q$ with $d^9 - d = c$. Then $\mathbb{F}_q(d)$ is a degree-6 extension of \mathbb{F}_q .

Let $e = F(d)$ so that

$$e = \frac{(c^8 + 1)^5}{c^{36}} \in \mathbb{F}_q.$$

Then d is a root of the rational function $F(z) - e$ in $\mathbb{F}_q(z)$, so d^q is another root of this function. By the reasoning from the proof of Lemma 5.2, we see that there is an element $\sigma \in G$ with $d^q = \sigma(d)$. Let $\bar{\sigma}$ denote the image of σ under the action of $\text{Gal}(\mathbb{F}_9/\mathbb{F}_3)$ on G . Then $(\bar{\sigma}\sigma)^3$ acts trivially on d , but no smaller power of $(\bar{\sigma}\sigma)$ acts trivially. It follows that $\bar{\sigma}\sigma$ has order 3. Enumerating the elements σ of G with this property, we find that there are elements τ and ρ of G such that $\sigma = \bar{\tau}\rho\tau^{-1}$ and

$$\rho \in \left\{ \begin{pmatrix} 1 & 1+i \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1+i & 1+i \\ 0 & 1+i \end{pmatrix} \right\}.$$

Let $d' = \tau^{-1}(d)$, so that d' is yet another root of $F(z) - e$, but now $(d')^q = \rho(d')$.

If $\rho(d') = d' + 1 + i$ then take $\bar{c} = (d')^9 - d'$. It is easy to check that $\bar{c} \in \mathbb{F}_q$ and that

$$\frac{(\bar{c}^8 + 1)^5}{\bar{c}^{36}} = \frac{(c^8 + 1)^5}{c^{36}}.$$

If $\rho(d') = id' + 1$ then take $\bar{c} = (1 + i)d'$. Then again we have $\bar{c} \in \mathbb{F}_q$, but now

$$\frac{(\bar{c}^8 + 1)^5}{\bar{c}^{36}} = -\frac{(c^8 + 1)^5}{c^{36}}.$$

□

REFERENCES

- [1] LEONARD M. ADLEMAN AND MING-DEH A. HUANG: *Primality testing and abelian varieties over finite fields*, Lecture Notes in Math. **1512**, Springer-Verlag, Berlin, 1992.
- [2] WIEB BOSMA, JOHN CANNON, AND CATHERINE PLAYOUST: The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997) 235–265.
- [3] EVERETT W. HOWE: Principally polarized ordinary abelian varieties over finite fields, *Trans. Amer. Math. Soc.* **347** (1995) 2361–2401.
- [4] EVERETT W. HOWE: Kernel of polarizations of abelian varieties over finite fields, *J. Algebraic Geom.* **5** (1996) 583–608.
- [5] EVERETT W. HOWE: Isogeny classes of abelian varieties with no principal polarizations, pp. 203–216 in: *Moduli of abelian varieties* (C. Faber, G. van der Geer and F. Oort, eds.), Progr. Math. **195**, Birkhäuser, Basel, 2001.
- [6] EVERETT W. HOWE: On the non-existence of certain curves of genus two, *Compos. Math.* **140** (2004) 581–592.
- [7] E.W. HOWE AND K.E. LAUTER: Improved upper bounds for the number of points on curves over finite fields, *Ann. Inst. Fourier (Grenoble)* **53** (2003) 1677–1737.
- [8] E.W. HOWE AND K.E. LAUTER: Corrigendum: “Improved upper bounds for the number of points on curves over finite fields,” in preparation, 2006.
- [9] EVERETT W. HOWE, DANIEL MAISNER, ENRIC NART, AND CHRISTOPHE RITZENTHALER: Principally polarized isogeny classes of abelian surfaces over finite fields, [arXiv:math.NT/0602650](https://arxiv.org/abs/math.NT/0602650).
- [10] EVERETT W. HOWE, ENRIC NART, AND CHRISTOPHE RITZENTHALER: Jacobians in isogeny classes of abelian surfaces over finite fields, preprint, 2006.
- [11] T. IBUKIYAMA, T. KATSURA, AND F. OORT: Supersingular curves of genus two and class numbers, *Compositio Math.* **57** (1986) 127–152.
- [12] J. IGUSA: Arithmetic variety of moduli for genus two, *Ann. of Math. (2)* **72** (1960) 612–649.
- [13] DANIEL MAISNER, Superficies abelianas como jacobianas de curvas en cuerpos finitos, thesis, Universitat Autònoma de Barcelona, 2004.
- [14] DANIEL MAISNER AND ENRIC NART WITH AN APPENDIX BY EVERETT W. HOWE: Abelian surfaces over finite fields as Jacobians, *Experiment. Math.* **11** (2002) 321–337.
- [15] D. MAISNER AND E. NART: Zeta functions of supersingular curves of genus two, *Canad. J. Math.*, to appear.
- [16] GARY MCGUIRE AND JOSÉ FELIPE VOLOCH: Weights in codes and genus 2 curves, *Proc. Amer. Math. Soc.* **133** (2005) 2429–2437.
- [17] A.-E. PELLET: Sur la décomposition d’une fonction entière en facteurs irréductibles suivant un module premier p , *C. R. Acad. Sci. Paris* **86** (1878) 1071–1072.
- [18] HANS-GEORG RÜCK: Abelian surfaces and Jacobian varieties over finite fields, *Compositio Math.* **76** (1990) 351–366.
- [19] JEAN-PIERRE SERRE: *Rational points on curves over finite fields*, unpublished notes by Fernando Q. Gouvêa of lectures at Harvard University, 1985.
- [20] NORIKO YUI: On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$, *J. Algebra* **52** (1978) 378–410.
- [21] YURI G. ZARHIN: Non-supersingular hyperelliptic Jacobians, *Bull. Soc. Math. France* **132** (2004) 617–634.
- [22] YURI G. ZARHIN: Homomorphisms of abelian varieties, pp. 189–215 in: *Arithmetic, Geometry and Coding Theory (AGCT 2003)* (Y. Aubry and G. Lachaud, eds.), Sémin. Congr. **11**, Soc. Math. France, Paris 2005.

CENTER FOR COMMUNICATIONS RESEARCH, 4320 WESTERRA COURT, SAN DIEGO, CA 92121-1967, USA.

E-mail address: `however@alumni.caltech.edu`

URL: `http://www.alumni.caltech.edu/~however/`